Retroactively estimating system clock skew from stored web browser cookies

Contents

Time. It matters.

John is a suspect in a fraud case – supposedly, he has tampered with the electronic cash register (PC software) in the grocery shop where he is employed.
John claims that he did no such thing and that some other person working the next shift must have been responsible.

Time. It matters.

John is a suspect in a fraud case – supposedly, he has tampered with the electronic cash register (PC software) in the grocery shop where he is employed.
John claims that he did no such thing and that some other person working the next shift must have been responsible.

A forensic investigation shows that the fraudulent records were timestamped 10:32.
An investigation of security camera footage shows John leaving the store premises at 10:30.

Time. It matters.

John is a suspect in a fraud case – supposedly, he has tampered with the electronic cash register (PC software) in the grocery shop where he is employed.
John claims that he did no such thing and that some other person working the next shift must have been responsible.

A forensic investigation shows that the fraudulent records were timestamped 10:32.
An investigation of security camera footage shows John leaving the store premises at 10:30.

...?

Time. It matters.

John is a suspect in a fraud case – supposedly, he has tampered with the electronic cash register (PC software) in the grocery shop where he is employed.
John claims that he did no such thing and that some other person working the next shift must have been responsible.

A forensic investigation shows that the fraudulent records were timestamped 10:32.
An investigation of security camera footage shows John leaving the store premises at 10:30.

$\rightarrow$ *What was the skew of the PC's clock with respect to the clock of the security camera?*

Time. It matters.

John is a suspect in a fraud case – supposedly, he has tampered with the electronic cash register (PC software) in the grocery shop where he is employed.
John claims that he did no such thing and that some other person working the next shift must have been responsible.

A forensic investigation shows that the fraudulent records were timestamped 10:32.
An investigation of security camera footage shows John leaving the store premises at 10:30.

$\rightarrow$ *What was the skew of the PC's clock with respect to the clock of the security camera? Or: what were their respective skews with respect to some universal clock?*

Skewed up clocks

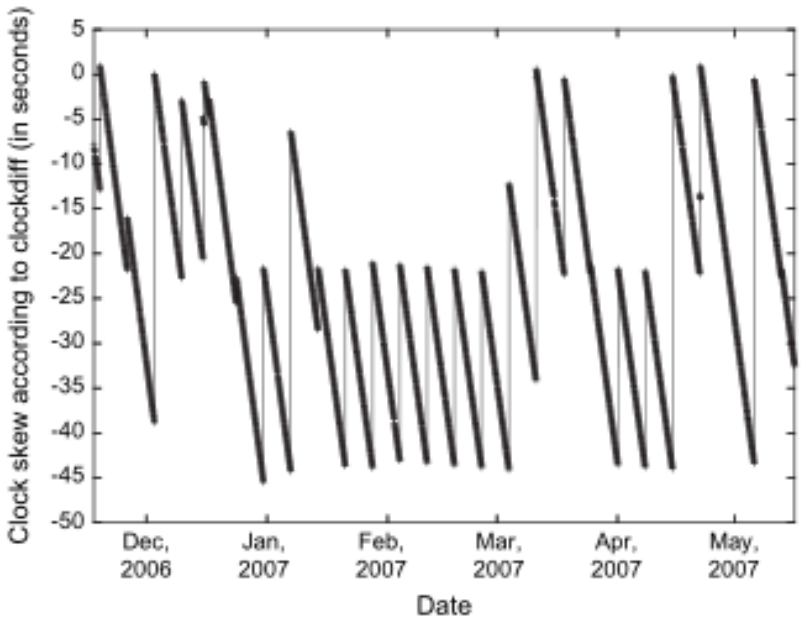


Fig. 17 – A clock with periodic jumps (sampled hourly).

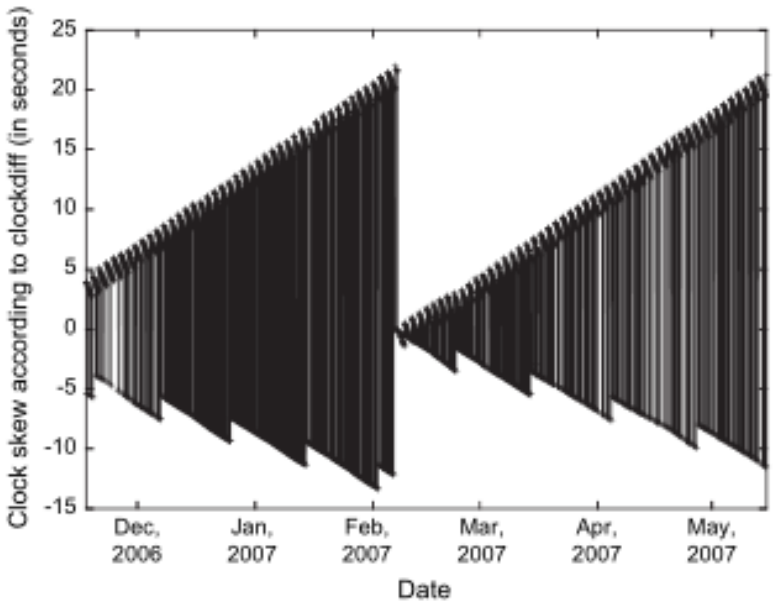
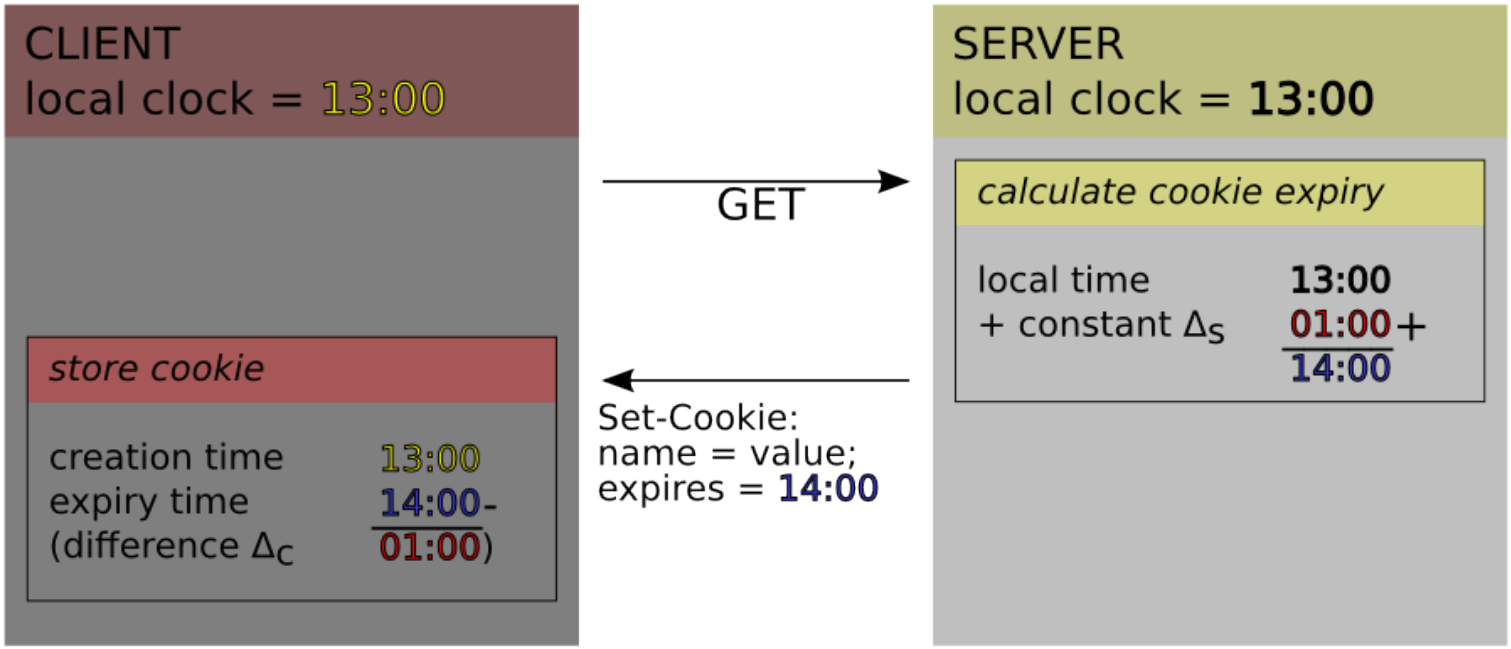


Fig. 19 – Two different hosts "sharing" an IP address?

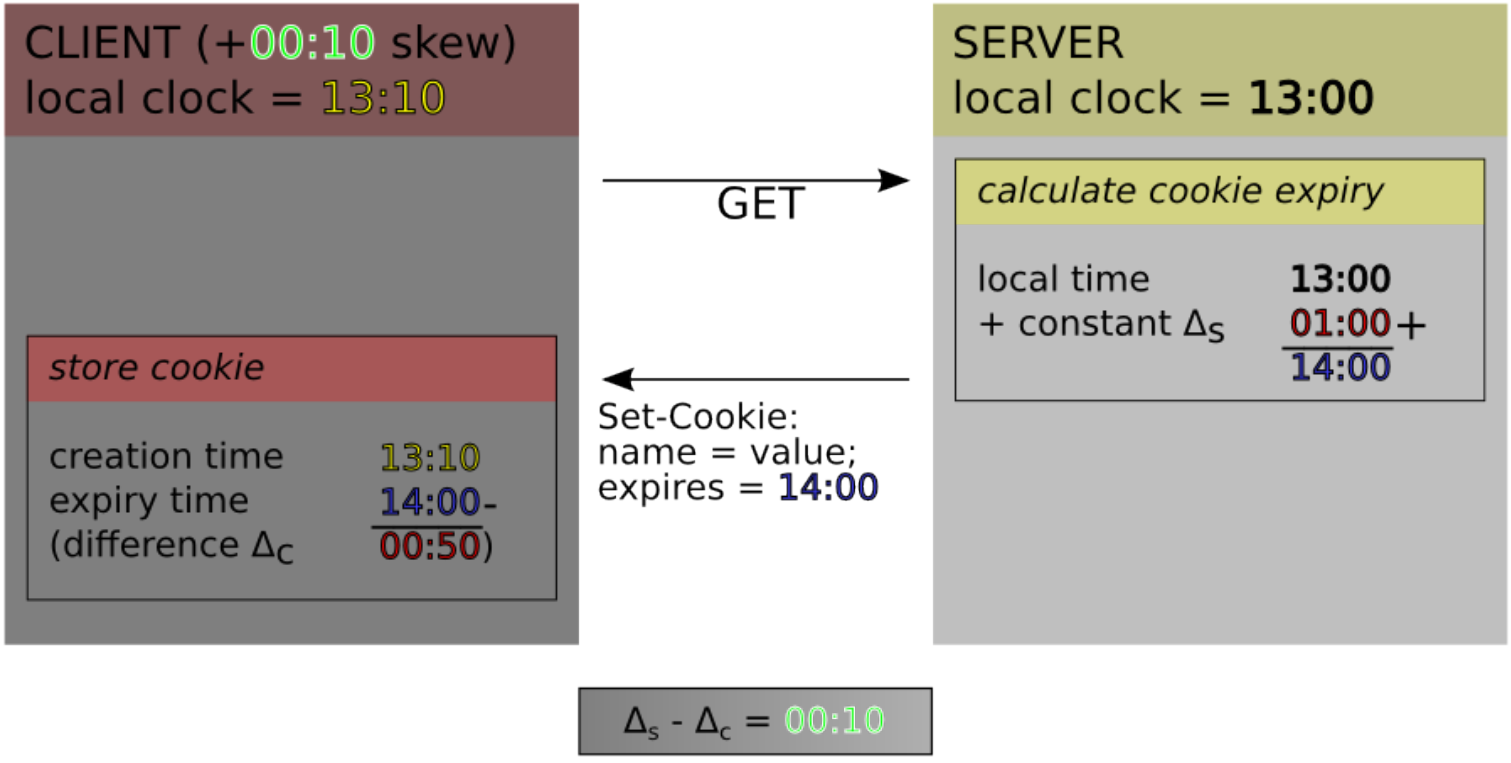
Server time ends up on your machine

Clocks in sync



Server time ends up on your machine

Client-side skew



Acquiring server deltas

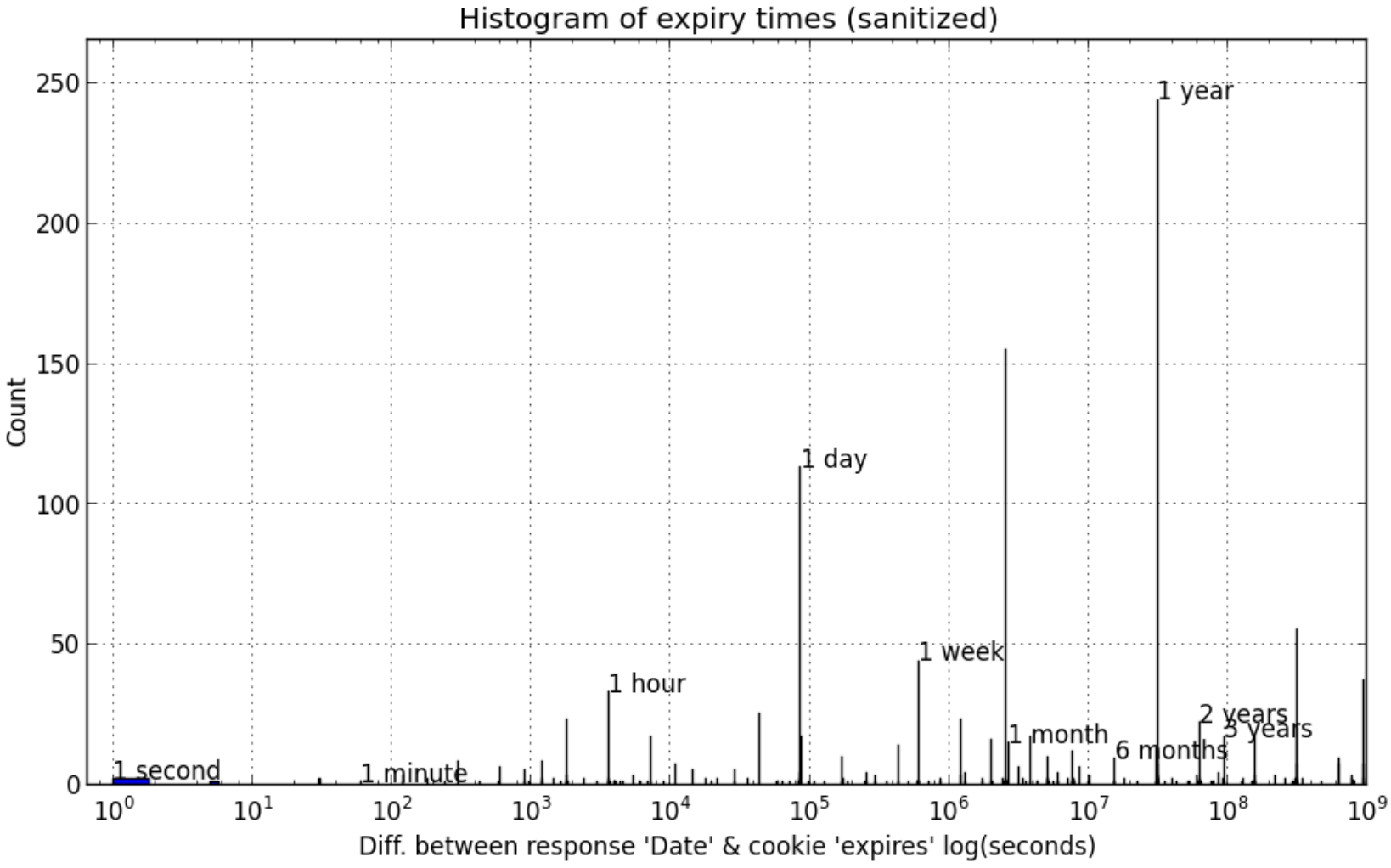
```
HTTP/1.0 200 OK
Server: nginx/1.2.0
Date: Fri, 21 Sep 2012 05:51:57 GMT
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie:
   anonymid=h7cvgx1h6is4h3;
   domain=.renren.com;
   path=/;
   expires=Wed,20-Sep-2017 05:51:57 GMT
```

Acquiring server deltas

```
HTTP/1.0 200 OK
Server: nginx/1.2.0
Date: Fri, 21 Sep 2012 05:51:57 GMT
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie:
   anonymid=h7cvgx1h6is4h3;
   domain=.renren.com;
   path=/;
   expires=Wed,20-Sep-2017 05:51:57 GMT
```

→ *Shodan Research HTTP Header Survey*

Acquiring server deltas



Demo time